International Journal of Scientific Research & Engineering Trends
Volume 5, Issue4, July-Aug-2019, ISSN (Online): 2395-566X

Three-Layer Privacy Preserving Cloud Storage Scheme in Fog Computing

M. Tech. Scholar M. Rajani
Department of Computer Science & Engineering
Gokula Krishna College of Engineering & Technology
Sullurupeta, Ap, India

Asst. Prof. B. Sai Sreenivas Rao
Department of Computer Science & Engineering
Gokula Krishna College of Engineering & Technology
Sullurupeta, Ap, India

Asst. Prof. T. Sujilatha
Department of Computer Science & Engineering
Gokula Krishna College of Engineering & Technology
Sullurupeta, Ap, India

Abstract - **Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In order to solve this problem, we propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.**

Keywords: **Cloud computing, cloud storage, fog computing, privacy protection.**

I. INTRODUCTION

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet to offer faster innovation, flexible resources, and economies of scale. Since the 21st century, computer technology has developed rapidly. Cloud computing, an emerging technology, was first proposed in SES 2006 (Search Engine Strategies 2006) by San Jose and defined by NIST (National Institute of Standards and Technology). Since it was proposed, cloud computing has attracted great attention from different sectors of society. Cloud computing has gradually matured through so many people's efforts. Then there are some cloud-based technologies deriving from cloud computing. Cloud storage is an important part of them.

With the rapid development of network bandwidth, the volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. Pursuing more powerful storage capacity, a growing number of users select cloud storage. Storing data on a public cloud server is a trend in the future and the cloud storage technology will become widespread in a few years. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together co-coordinately.
Nowadays there are a lot of companies providing a variety of cloud storage services, such as Drop box, Google Drive, icloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications, which in turn lead to their success in attracting humorous subscribers. However, cloud storage service still exist a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. For example, Apples icloud leakage event in 2014, numerous Hollywood actresses private photos stored in the clouds were stolen. This event caused uproar, which was responsible for the users' anxiety about the privacy of their data stored in cloud server. As shown in Fig. 1, user uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data.

In consequence, user does not actually control the physical storage of their data, which results in the separation of ownership and management of data. The

© 2019 IJSRET

CSP can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss.

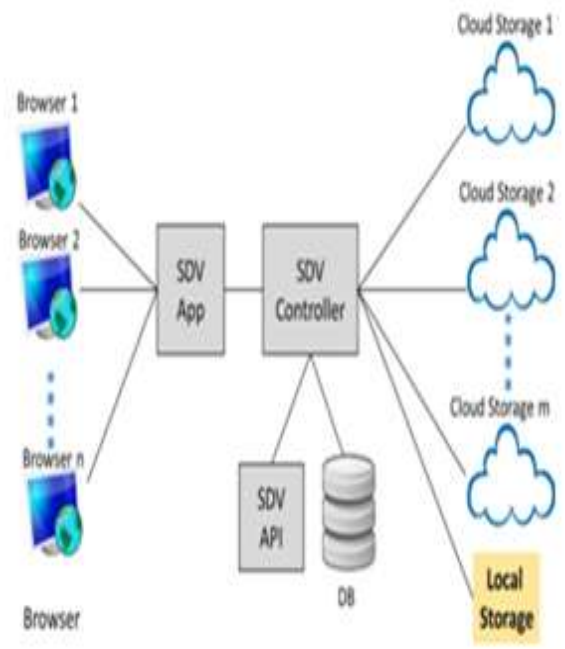

Fig.1. Traditional cloud storage structure.

In consequence, user does not actually control the physical storage of their data, which results in the separation of ownership and management of data. The CSP can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss.

Traditional secure cloud storage solutions for the above problems are usually focusing on access restrictions or data encryption. These methods can actually eliminate most part of these problems. However, all of these solutions cannot solve the internal attack well, no matter how the algorithm improves. Therefore, we propose a TLS scheme based on fog computing model and design a Hash-Solomon code based on Reed-Solomon code. Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability. In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine. Besides, depending on the property of the Hash-Solomon code, the scheme can ensure the original data cannot be recovered by partial data. On another hand, using Hash-Solomon code will produce a portion of redundant data blocks which will be used in decoding procedure. Increasing the number of redundant blocks can increase the reliability of the storage, but it also results in additional data storage.

By reasonable allocation of the data, our scheme can really protect the privacy of user' data. The Hash-Solomon code needs complex calculation, which can be assisted with the Computational Intelligence (CI). Paradigms of CI have been successfully used in recent years to address various challenges, for example, the problems in Wireless sensor networks (wsns) field. CI provides adaptive mechanisms that exhibit intelligent behavior in complex and dynamic environments like wins. Thus in our paper, we take advantage of CI to do some calculating works in the fog layer. Compared with traditional methods, our scheme can provide a higher privacy protection from interior, especially from the csps.

II. RELATED WORK

The importance of security in cloud storage has attracted a lot of attention no matter in academe or industry. There are a lot of researches about secure cloud storage architectures in recent years. In order to solve the privacy issue in cloud computing, use variety encryption policies in different positions. Solve the privacy problem with the help of auditing or building their own secure framework. However, there is a common defect in these researches. Once the CSP is un-trusted, all of these schemes are invalid. They cannot resist internal attacks or prevent the CSP from selling user's data to earn illegal profit. The private data will be decoded once malicious attackers get it no matter how advanced the encryption technologies are because user's data was integrally stored in cloud server. Therefore, we propose a new secure cloud storage scheme in this paper. By dividing file with specific code and combining with TLS framework based on fog computing model, we can achieve high degree privacy protection of data. It does not mean that we abandon the encryption technology. In our scheme encryption also help us to protect fine-grained secure of the data.

III. EXISTING SYSTEM

In existing system, data has been partitioned and stored in three storage servers such as cloud server, fog server and local server by hash- Solomon code algorithm. One important thing is that the third party doesn't have the knowledge about our data partitioning. The Cloud server contains 80% of unimportant information, the Fog server contains 15% of most important information and the Local server contains 5% of important information. If hacker hacks the data in any one these layers, either he/she will modify the data or delete the data. Hence the user will lose that data. This is the major disadvantage.

© 2019 IJSRET

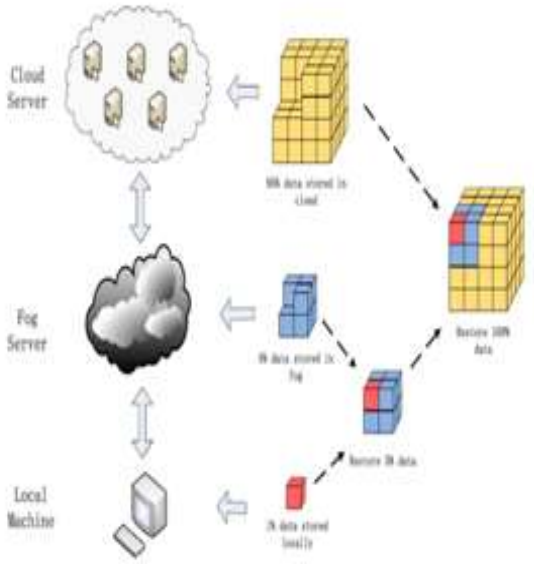

Fig. 2. Illustration of Three-Layer storage framework based on fog computing.

IV. PROPOSED METHOD

The proposed frame work can both take full advantage of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.

- The security degree is an important metric to measure the quality of cloud storage system.
- Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy.
- TLS frame- work based on fog computing model is used in proposed system.

  The TSL framework can give user a certain power of management and effectively protect user's privacy.
  This paper implements a framework called bucket to secure and restore the lost data. Bucket is like a mirror, whatever data has been implemented by the user the data will be automatically stored in the bucket framework. The proposed algorithm data comparison in three layers and matched data are stored in bucket.
- **Secure Cloud Storage Based On Fog Computing**

  The security degree is an important metric to measure the quality of cloud storage system. Furthermore, data security is the most important part in cloud storage security and it includes three aspects: data privacy, data integrity and data availability. Ensuring data privacy and integrity has always been the focus of relevant researches. On another hand, data privacy is also the most concerned part of the users. From a business perspective, company with high security degree will attract more users. Therefore improving security is a crucial goal no matter in academia or business. In this section, we will explain elaborate how the TLS framework protects the data privacy, the implementation details of work flow and the theoretical safety and efficiency analysis of the storage scheme.
- **B. Three-Layer Privacy Preserving Cloud Storage Scheme Based On Fog Computing Model**

  In order to protect user's privacy, we propose a TLS framework based on fog computing model. The TSL framework can give user a certain power of management and effectively protect user's privacy. As mentioned, the interior attack is difficult to resist. Traditional approaches work well in solving outside attack, but when CSP itself has problems, traditional ways are all invalid. Different from the traditional approaches, in our scheme, user's data is divided into three different-size parts with encoding technology. Each of them will lack a part of key information for confidentiality. The three different privacy preserving layers are Cloud server, Fog server and Local server. A complete data is now partitioned and stored into three different layers. The ratio of the partition of data is major part of the data is stored in the cloud server; neither high nor low range of data is stored in the fog server and finally lower amount of local server. When the data required it can be combined into a single data using pattern matching method.

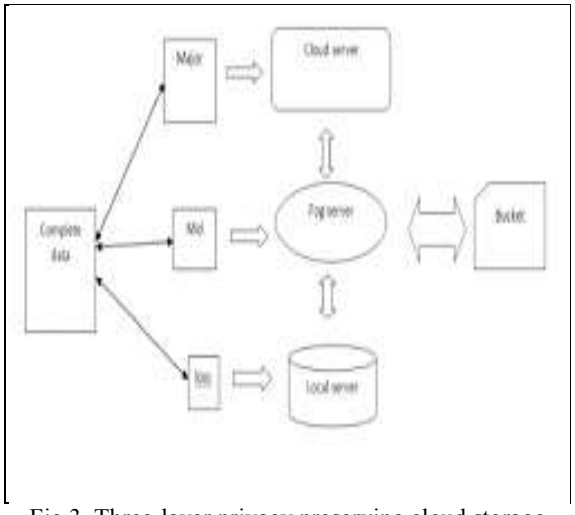

Fig.3. Three-layer privacy preserving cloud storage architecture.

© 2019 IJSRET

- **Fog Computing**
  Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer.
  Fog computing layer can perform critical data transmission to cloud server. And finally the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer.

V. MODULE DESCRIPTION

- **Registration module**
  This module is used for the user to register their login id by providing the minimal information. User want enter their minimal information such as mail id, name, mobile number, password which is used for further logins. So they can login to the website.
- **Login Module**
  In this module, user can login to the website by registered login id and a valid password. If it is not a valid user he/she cannot login to it. Only the authenticated users can login and use the website.
- **Storage Module**
  In this module, user can store their files into three different storage servers. The storage servers are cloud server, fog server and local server. In cloud server we store 80% of data. In fog server we store sensitive 15% of data. In local server we store 5% of data.
- **Recovery Module**
  In this module, user can recover their files from three different storage servers. By using BCH algorithm, if the data matched with these three layers of data then it will be stored in the bucket. If the data has been hacked in any one of the layers, the user can easily recover it from bucket framework.

VI. DOWNLOAD PROCEDURE

When user wants to download his file from the cloud server, the procedure is shown in Fig. 4. Firstly, cloud server receives user's request and then integrates the data in different distributed servers. After integration, cloud server sends the 95% data to the fog server.

Secondly, the fog server receives the data from the cloud server. Combining with the 4% data blocks of fog server and the encoding information, we can recover 99% data. Then the fog server returns the 99% data to the user. Thirdly, the user receives the data from fog server. User can get the complete data by repeating the above steps.

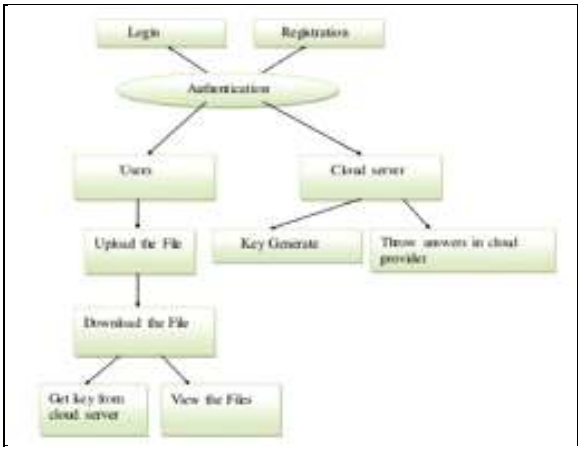

Fig.4. Proposed model download steps.

VII. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a bucket framework based on fog computing model and design a BCH Code algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible.

VIII. FUTURE ENHANCEMENT

As the cloud storage scheme based on fog computing is done by the mentioned algorithms, it can further developed by using some other algorithms to reduce the lines of code and to reduce the time complexity.

REFERENCES

[1]. T. Wang, J. Y. Zhou, and X. L. Chen are with the Department of Computer Science and Technology, Huaqiao University, Xiamen 361021, China (e-mail:cs_tianwang@163.com;zhoujiyuan1994@foxmail.com; adamwt@163.com).
[2]. P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.
[3]. Secure and Privacy-Preserving Data Storage Service in Public Cloud Li Hui1, Sun Wenhai1, Li

Fenghua2, And Wang Boyang1Vol. 51, no. 7, pp. 1397–1409, 2014.
[4]. L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Dataacquis. Process., vol. 31, no. 3, pp. 464–472, 2016.
[5]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp. 2594–2608, Nov. 2016.
[6]. Fog computing and its role in the internet of things F. Bonomi, R. Milito, J.Zhu, s.Addepalli vol. 11, no. 12, pp. 2706–2716, Dec. 2016.
[7]. A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities Jian shena. B,c, dengzhiliuc, junshenc, qi liua,c, xingmingsuna,c vol. 41 , pp. 219–230, 2017.

AUTHOR'S PROFILE

M.RAJANI Pursuing M.Tech at Gokula Krishna College of Engineering & Technology, Department of CSE, Sullurupeta, Nellore Dist.

B. SAI SREENIVAS RAO Working as an Assistant Professor in Gokula Krishna College of Engineering & Technology, Department of CSE, Sullurupeta, Nellore dist.

T.SUJILATHA Working as an Assistant Professor in Gokula Krishna College of Engineering & Technology, Department of CSE, Sullurupeta, Nellore dist. She is having 6 years of teaching experience in engineering colleges, She is interested in Networking and Cloud computing.

© 2019 IJSRET